

EJ187645680US

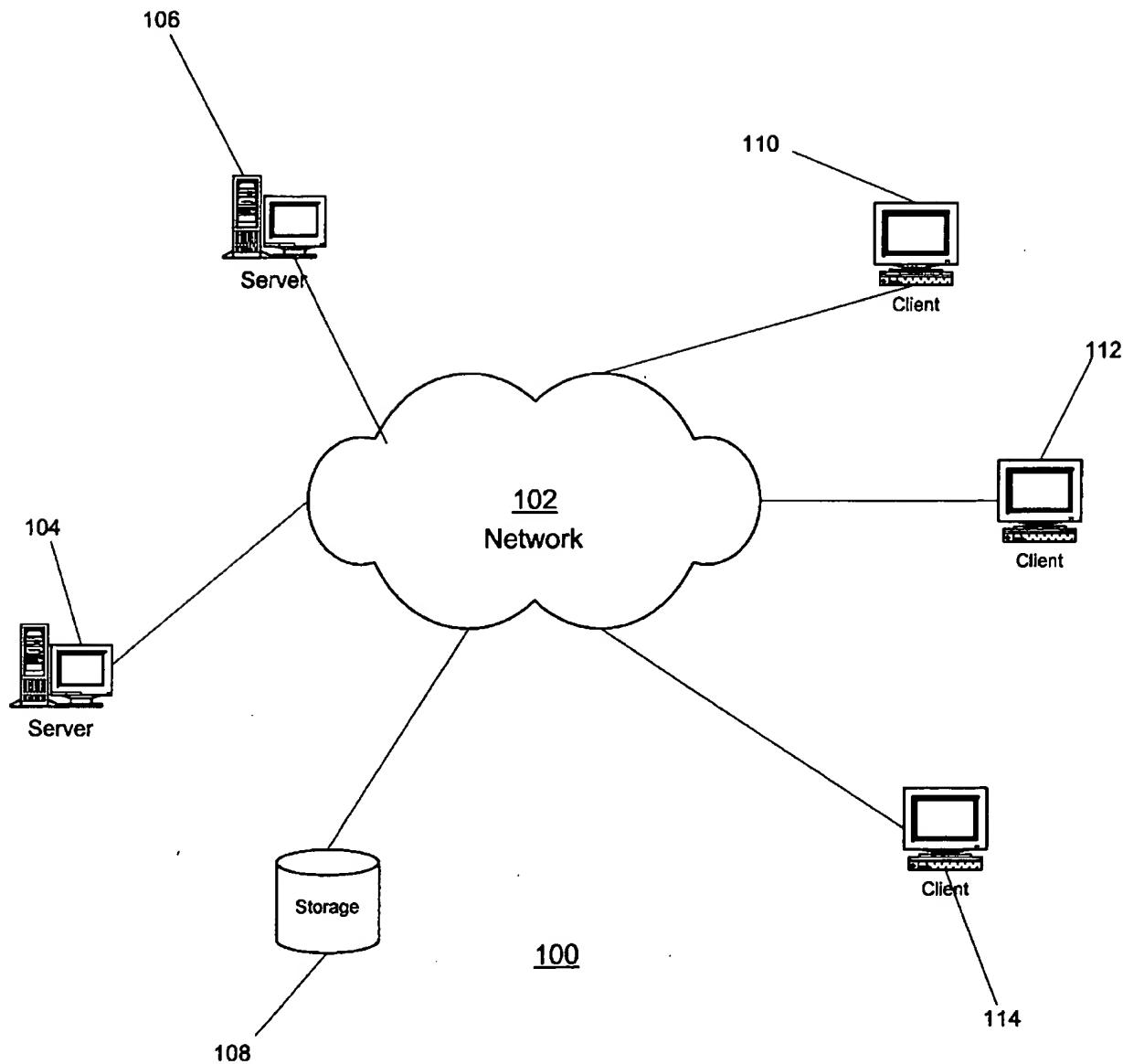


Figure 1

EnvelopedData Interface
AUS990880US1

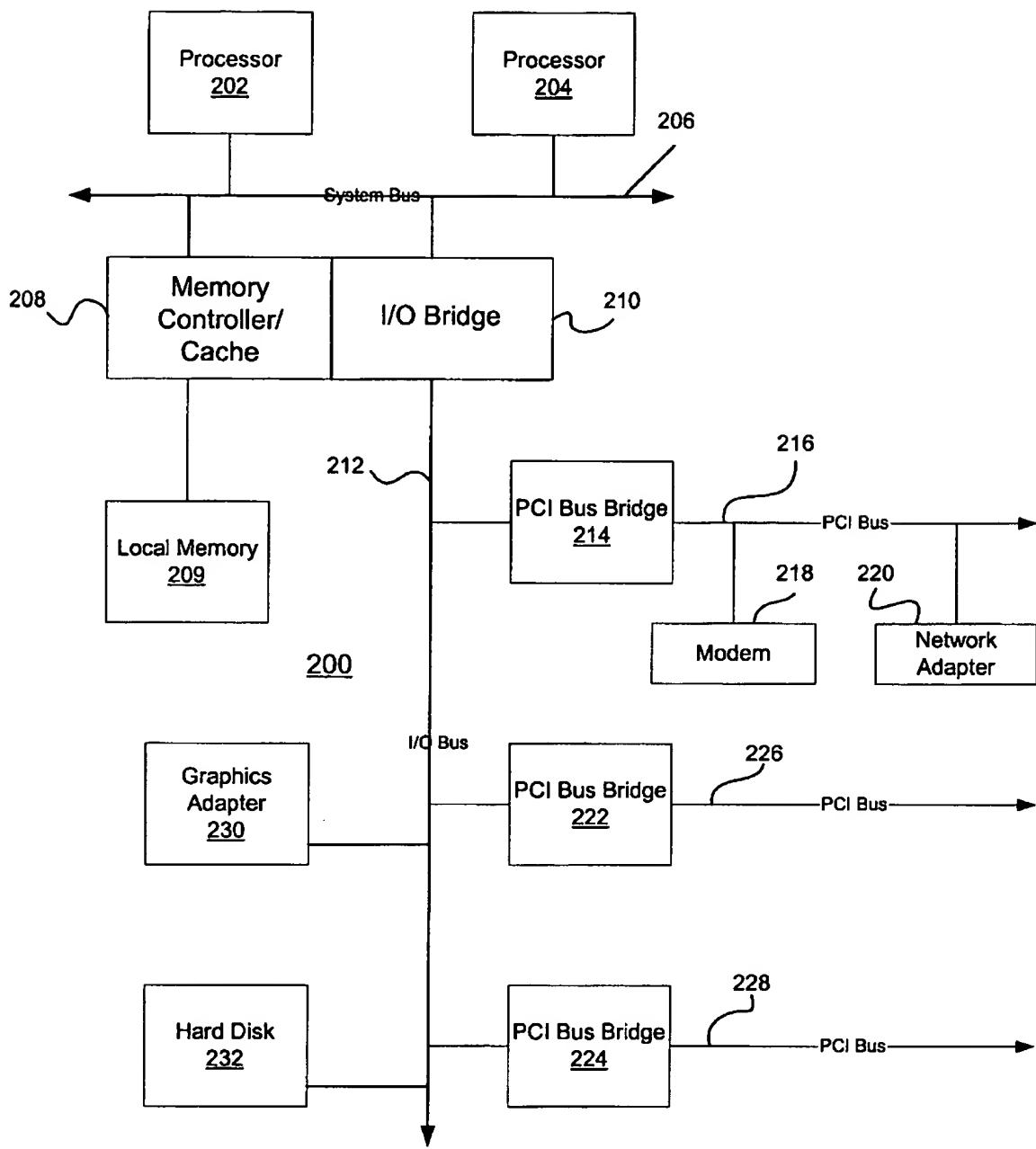
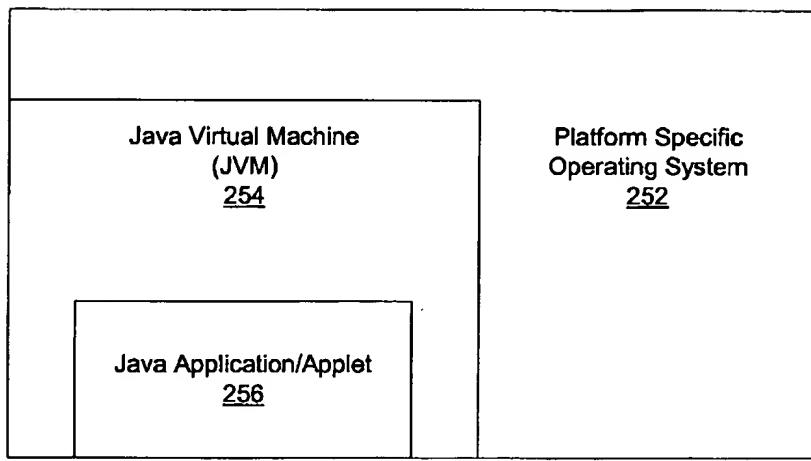


Figure 2A

EnvelopedData Interface
AUS990880US1



250

Figure 2B

AUS990880US1

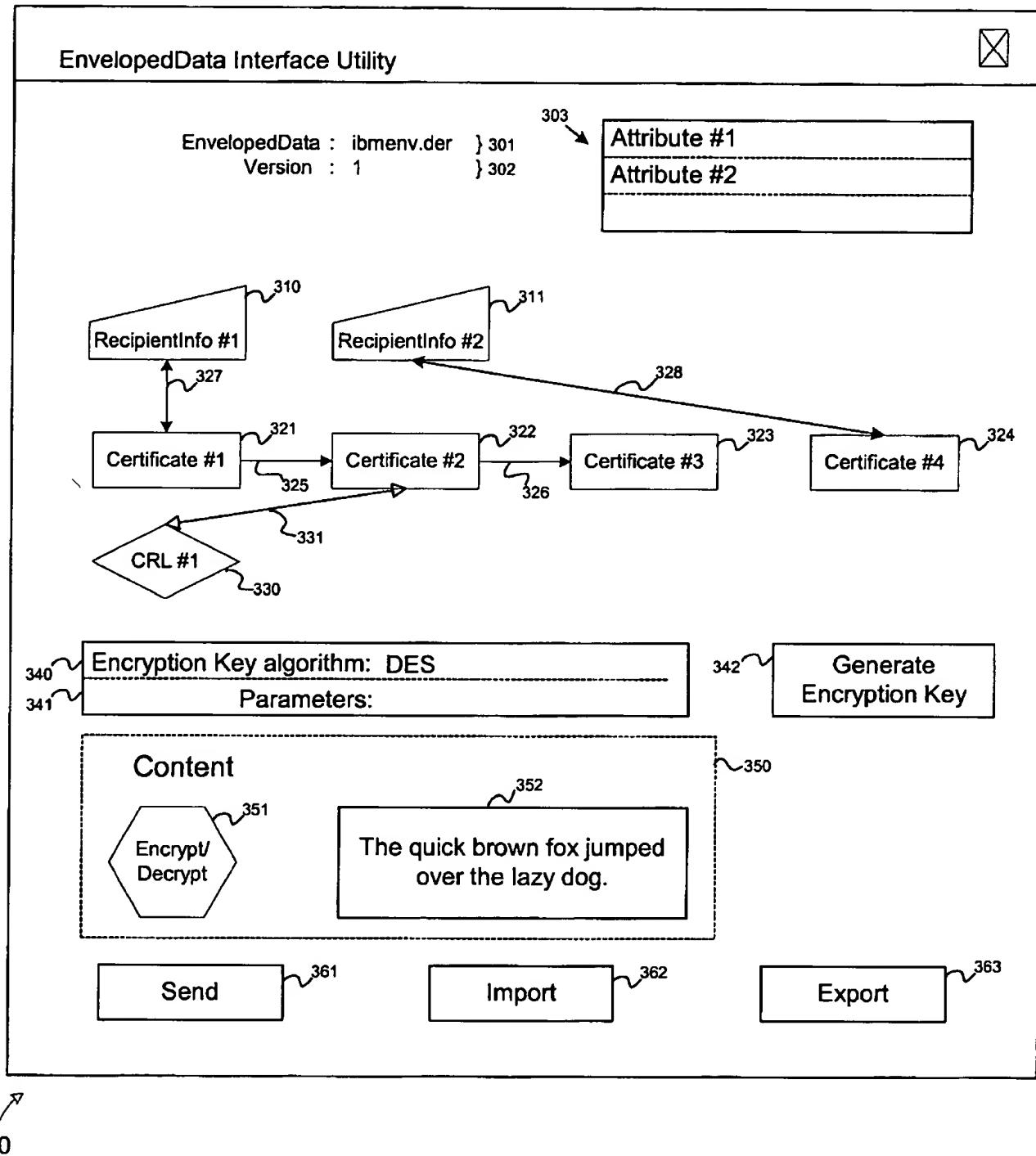


Figure 3

EnvelopedData Interface
AUS990880US1

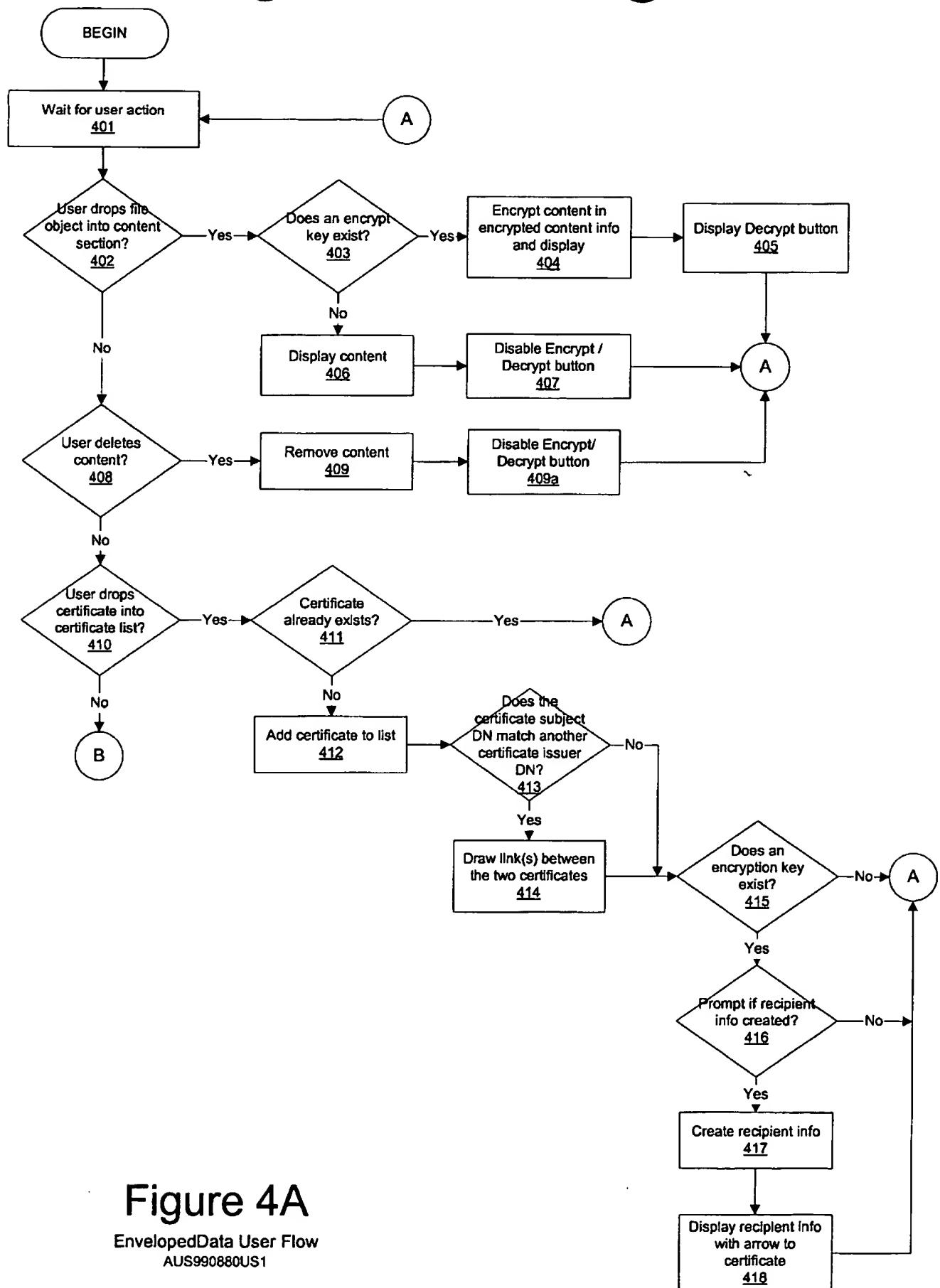


Figure 4B

EnvelopedData User Flow
AUS990880US1

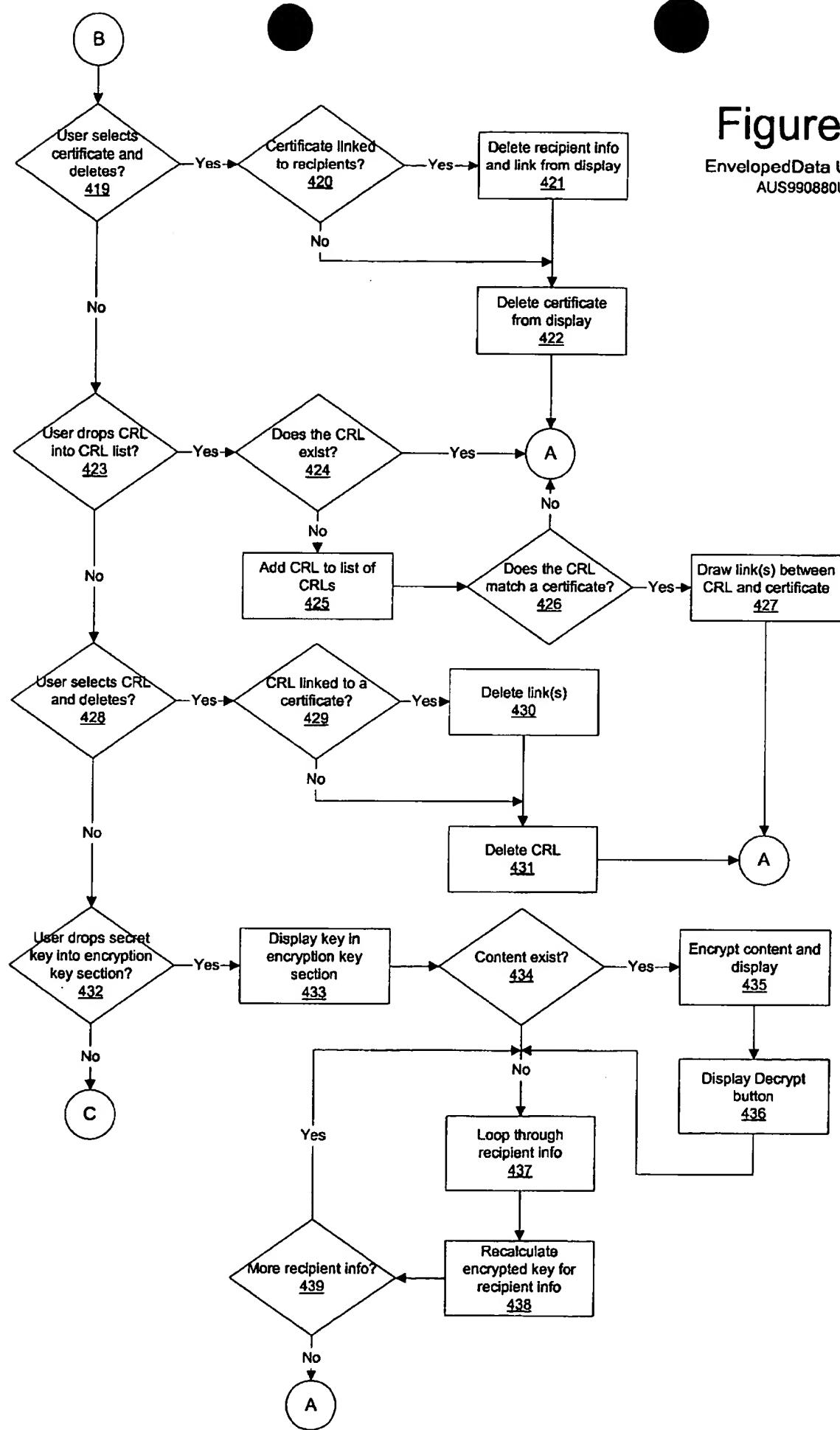
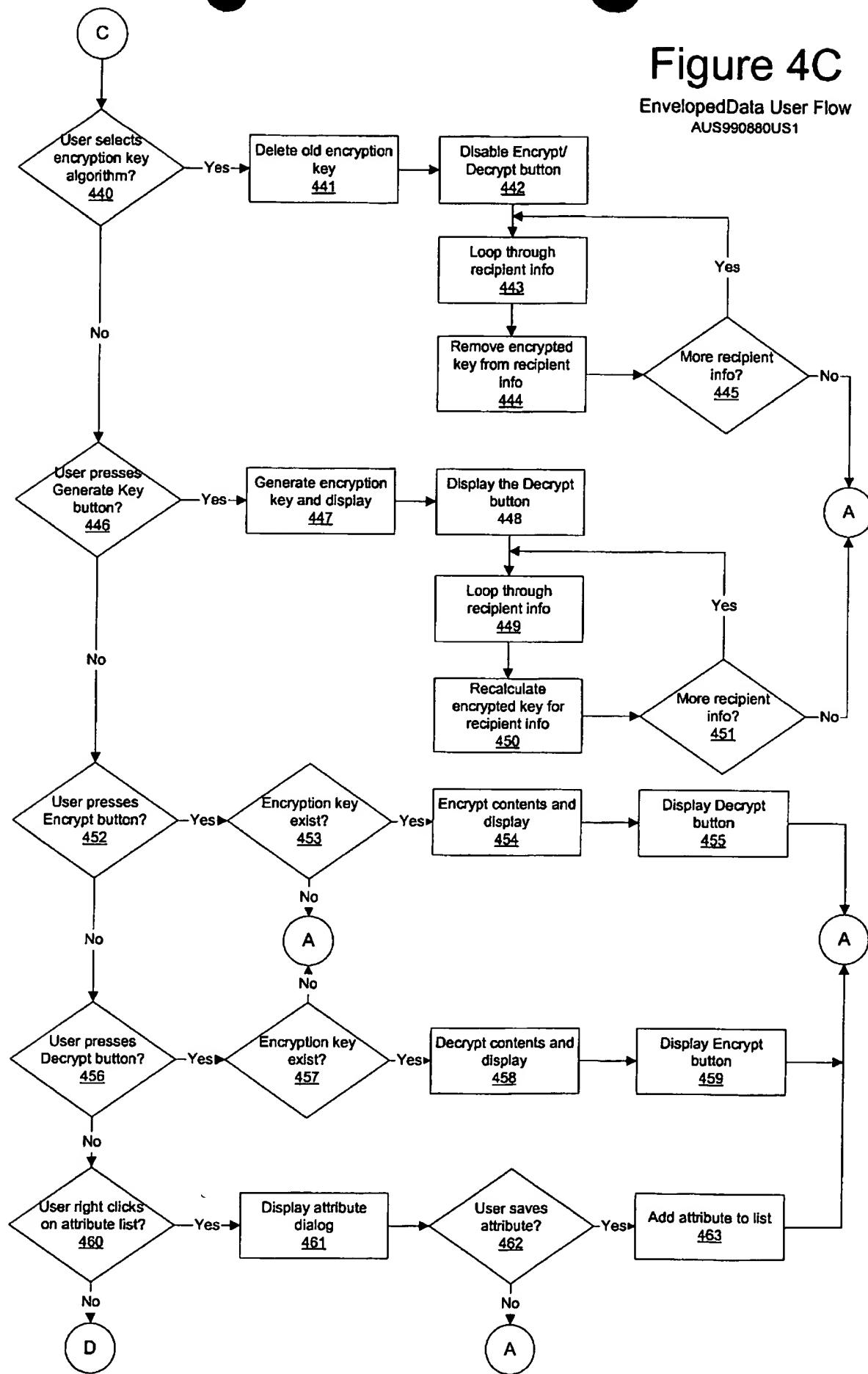


Figure 4C

EnvelopedData User Flow
AUS990880US1



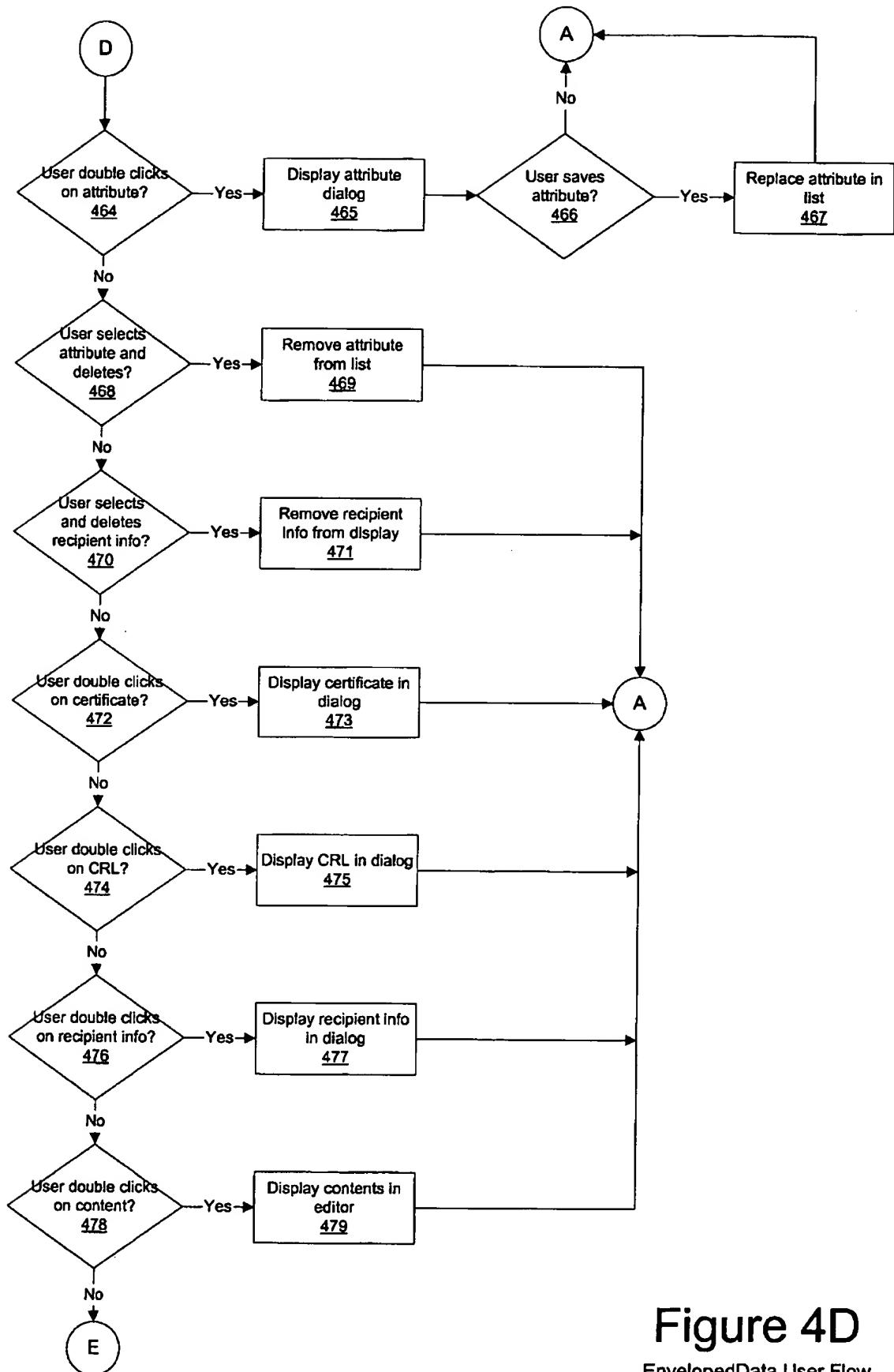
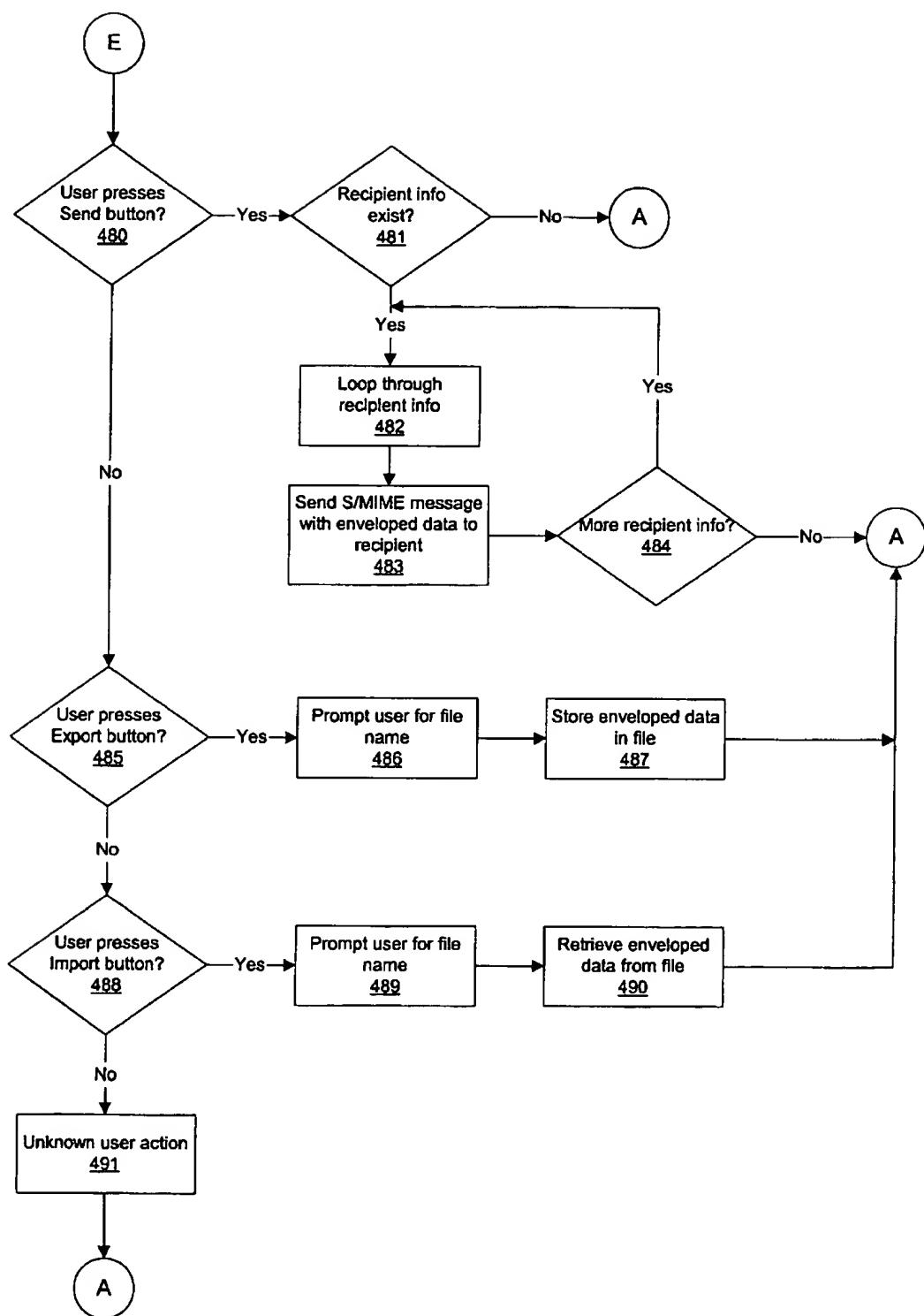


Figure 4D

EnvelopedData User Flow
AUS990880US1

Figure 4E

EnvelopedData User Flow
AUS990880US1



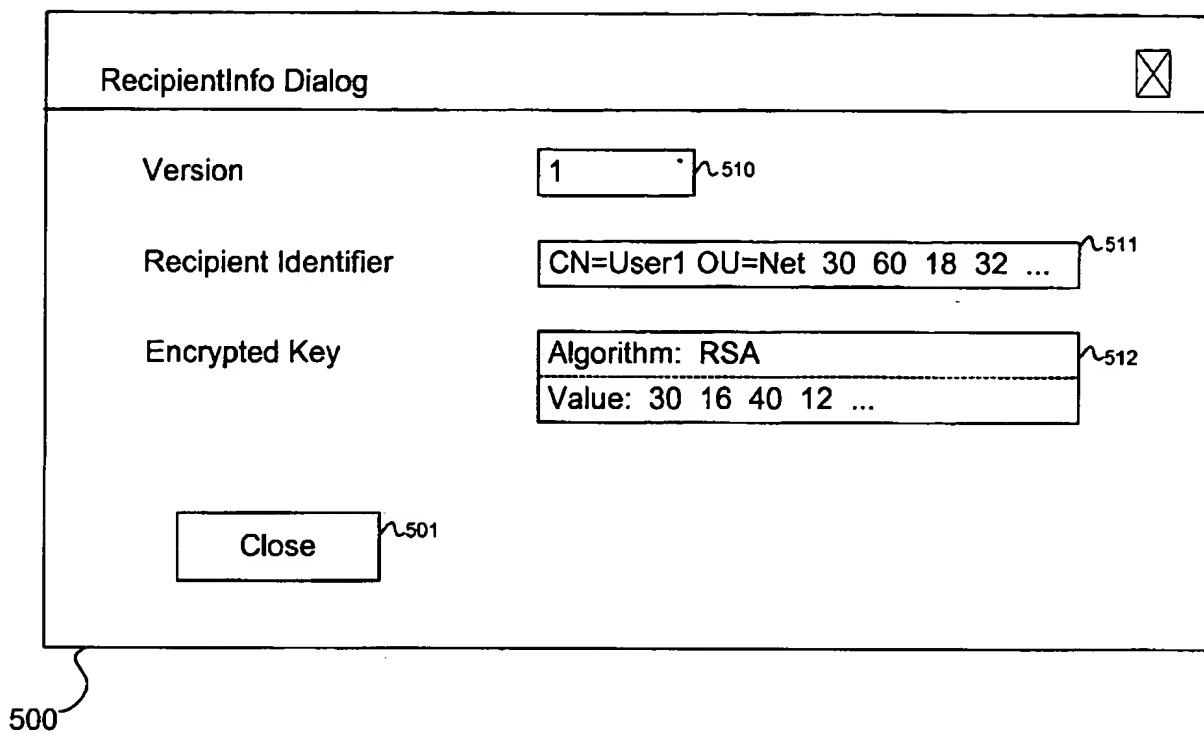


Figure 5A

AUS990880US1

```

RecipientInfo ::= CHOICE {
  ktri KeyTransRecipientInfo,
  kari [1] KeyAgreeRecipientInfo,
  kekri [2] KEKRecipientInfo }

KeyTransRecipientInfo ::= SEQUENCE {
  version CMSVersion, -- always set to 0 or 2
  rid RecipientIdentifier,
  keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
  encryptedKey EncryptedKey }

RecipientIdentifier ::= CHOICE {
  issuerAndSerialNumber IssuerAndSerialNumber,
  subjectKeyIdentifier [0] SubjectKeyIdentifier }
  
```

Figure 5B

AUS990880US1

Attribute Dialog X

Name 610

Type 611

Value 612

601

602

600

Figure 6
AUS990880US1

700 ↗

Certificate Dialog

Version	3	710	Private Key	720	
Serial Number	31 40 60 14 ...	711			
IssuerDN	CN=User1 OU=Net	712			
Issuer Serial Number	40 31 14 56 ...	713			
SubjectDN	CN=Signer OU=Net	714			
Validity Period	12/01/1999	715	to	11/30/2000	716
Public Key	Algorithm: RSA	717			
	Value: 30 16 40 12 ...	718			
Signature	Algorithm: MD5 with RSA	719			
	Value: 30 20 18 36 ...	720			
Extended Attributes	Algorithm: Policies 5	721			
	Value: Basic Constraints	722			

Close 701

Figure 7

AUS990880US1

800

CRL Dialog

Version 810

Issuer DN 812

Update Period 814 next 815

Extensions 816

Signature Algorithm: MD5 with RSA 817
Value: 30 40 32 ...

Revoked Certificate List 818

801

Figure 8

AUS990880US1